

(2) Whether the cost of collecting the information from the individual is unreasonable when compared with the cost of collecting it from a third party;

(3) Whether there is a risk that information requested from the third parties, if inaccurate, could result in an adverse determination to the individual concerned;

(4) Whether the information, if supplied by the individual, would have to be verified by a third party; or

(5) Whether provisions can be made for verification by the individual of information collected from third parties.

(e) Employees whose duties require handling of records subject to the Act shall, at all times, take care to protect the integrity, security and confidentiality of these records.

(f) No employee of the section may alter or destroy a record subject to the Act unless (1) such alteration or destruction is properly undertaken in the course of the employee's regular duties or (2) such alteration or destruction is required by a decision of the Commissioner or the decision of a court of competent jurisdiction.

**§ 1101.4 Reports on new systems of records; computer matching programs.**

(a) Before establishing any new systems of records, or making any significant change in a system of records, the Section shall provide adequate advance notice to:

(1) The Committee on Government Operations of the House of Representatives;

(2) The Committee on Governmental Affairs of the Senate; and

(3) The Office of Management and Budget.

(b) Before participating in any computerized information "matching program," as that term is defined by 5 U.S.C. 552a(a)(8) the Section will comply with the provisions of 5 U.S.C. 552a(o), and will provide adequate advance notice as described in § 1101.4(a) above.

**§ 1101.5 Security, confidentiality and protection of records.**

(a) The Act requires that records subject to the Act be maintained with appropriate administrative, technical and

physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

(b) When maintained in manual form (typed, printed, handwritten, etc.) records shall be maintained, at a minimum, subject to the following safeguards, or safeguards affording comparable protection:

(1) Areas in which the records are maintained or regularly used shall be posted with an appropriate warning stating that access to the records is limited to authorized persons. The warning shall also summarize the requirements of § 1101.3 and state that the Act contains a criminal penalty for the unauthorized disclosure of records to which it applies.

(2) During working hours: (i) The area in which the records are maintained or regularly used shall be occupied by authorized personnel or (ii) access to the records shall be restricted by their storage in locked metal file cabinets or a locked room.

(3) During non-working hours, access to the records shall be restricted by their storage in locked metal file cabinets or a locked room.

(4) Where a locked room is the method of security provided for a system, that security shall be supplemented by: (i) Providing lockable file cabinets or containers for the records or (ii) changing the lock or locks for the room so that they may not be opened with a master key. For purposes of this paragraph, a master key is a key which may be used to open rooms other than the room containing records subject to the Act, unless those rooms are utilized by officials or employees authorized to have access to the records subject to the Act.

(5) Personnel handling personal information during routine use will ensure that the information is properly controlled to prevent unintentional or unauthorized disclosure. Such information will be used, held, or stored only

## § 1101.6

## 22 CFR Ch. XI (4-1-07 Edition)

where facilities or conditions are adequate to prevent unauthorized or unintentional disclosure.

(c) When the records subject to the Act are maintained in computerized form, safeguards shall be utilized based on those recommended in the National Bureau of Standard's booklet "Computer Security Guidelines for Implementing the Privacy Act of 1974" (May 30, 1975), and any supplements thereto, which are adequate and appropriate to assuring the integrity of the records.

### § 1101.6 Requests for access to records.

(a) Any individual may submit an inquiry to the Section to ascertain whether a system of records contains a record pertaining to him or her.

(b) The inquiry should be made either in person or by mail addressed to the PA Officer, United States Section, International Boundary and Water Commission, 4171 North Mesa, Suite C-310, El Paso, TX 79902-1422. The PA Officer shall provide assistance to the individual making the inquiry to assure the timely identification of the appropriate systems of records. The office of the PA Officer is located in Suite C-316 and is open to an individual between the hours of 8 a.m. and 4:30 p.m., Monday through Friday (excluding holidays).

(c) Inquiries submitted by mail should be marked "PRIVACY ACT REQUEST" on the bottom left-hand corner of the envelope.

(d) The letter should state that the request is being made under the Privacy Act.

(e) Inquiries concerning whether a system of records contains a record pertaining to an individual should contain the following:

(1) Name, address and telephone number (optional) of the individual making the inquiry;

(2) Name, address and telephone number (optional) of the individual to whom the record pertains, if the inquiring individual is either the parent of a minor or the legal guardian of the individual to whom a record pertains;

(3) A certified or authenticated copy of documents establishing parentage or guardianship;

(4) Whether the individual to whom the record pertains is a citizen of the

United States or an alien lawfully admitted for permanent residence into the United States;

(5) Name of the system of records, as published in the FEDERAL REGISTER;

(6) Location of the system of records, as published in the FEDERAL REGISTER;

(7) Such additional information as the individual believes will or might assist the Section in responding to the inquiry and in verifying the individual's identity (for example: date of birth, place of birth, names of parents, place of work, dates of employment, position title, etc.);

(8) Date of inquiry; and

(9) Signature of the requester.

The Section reserves the right to require compliance with the identification procedures appearing at paragraph (f) of this section where conditions warrant.

(f) The requirement for identification of individuals seeking access to records are as follows:

(1) In person: Each individual making a request in person shall be required to present satisfactory proof of identity. The means of proof, in the order of preference and priority, are:

(i) A document bearing the individual's photograph (for example, driver's license, passport or military or civilian identification card);

(ii) A document bearing the individual's signature, preferably issued for participation in a federally sponsored program (for example, Social Security card, unemployment insurance book, employer's identification card, national credit card and professional, craft or union membership card); and

(iii) A document bearing either the photograph or the signature of the individual, preferably issued for participation in a federally sponsored program (for example, Medicaid card). In the event the individual can provide no suitable documentation of identity, the Section will require a signed statement asserting the individual's identity and stipulating that the individual understands the penalty provision of 5 U.S.C. 552a(i)(3).

(2) Not in person: If the individual making a request does not appear in person before the PA Officer, a certificate of a notary public or equivalent